

# Umbrellaダッシュボードでのネットワークトンネルの非アクティブの解決

## 内容

---

[はじめに](#)

[問題](#)

[トラブルシュート](#)

---

## はじめに

このドキュメントでは、Umbrellaダッシュボードで非アクティブとして表示されるネットワークトンネルをトラブルシューティングする方法について説明します。

## 問題

ネットワークトンネルを追加すると、トンネルはUmbrellaダッシュボードに非アクティブとして表示されます。

## トラブルシュート

1. ネットワークトンネルをアクティブ化するために、デフォルトのCloud-Delivered Firewall(CDFW)ポリシーのロギングを有効にします。デフォルトのCloud-Delivered Firewall(CDFW)ポリシーのロギングが有効になっている場合にのみ、ネットワークトンネルは「アクティブ」と表示されます。

Cisco Umbrella

Overview
Deployments
Policies
Management
DNS Policies
Firewall Policy
Web Policies
Policy Components
Destination Lists
Content Categories
Application Settings
Tenant Controls
Security Settings
Block Page Appearance
Integrations
Selective Decryption Lists
Reporting
Admin
Investigate
Demo User
dCloud Demo (cisco)

Policies / Management
Firewall Policy

Use this policy to control network traffic based on IP, port, and protocol. Rules are evaluated from the top down. For more information about Firewall Policy, view [Manage Firewall](#).

FILTERS

7 Total

| <input type="checkbox"/> | Priority | Name                           | Status  | Action | Applications                                  | Protocol | Source Criteria      | Destination Criteria | Hit Count    | Last Hit               |     |
|--------------------------|----------|--------------------------------|---------|--------|-----------------------------------------------|----------|----------------------|----------------------|--------------|------------------------|-----|
| <input type="checkbox"/> | 1        | Umbrella Branch - App Blocking | Enabled | Block  | bittorrent<br>bittorrent-networking<br>3 more | Any      | Any IPs<br>Any Ports | Any IPs<br>Any Ports | 0/24hrs      | Jul 18, 2020 - 06:41pm | ... |
| <input type="checkbox"/> | 2        | Umbrella HQ - Port Blocking    | Enabled | Block  | Any Application                               | Any      | Any IPs<br>Any Ports | Any IPs<br>3 Ports   | 318.0 /24hrs | Jul 21, 2020 - 11:14pm | ... |
| <input type="checkbox"/> | 3        | Umbrella HQ - IP Blocking      | Enabled | Block  | Any Application                               | Any      | Any IPs<br>Any Ports | 1 IP<br>Any Ports    | 0/24hrs      | Jun 29, 2020 - 06:10pm | ... |
| <input type="checkbox"/> | 4        | Allow Umbrella Resolvers       | Enabled | Allow  | Any Application                               | Any      | Any IPs<br>Any Ports | 2 IPs<br>Any Ports   | 25.2 k/24hrs | Jul 21, 2020 - 11:16pm | ... |
| <input type="checkbox"/> | 5        | Block SSH to SQL Server        | Enabled | Block  | Any Application                               | Any      | Any IPs<br>Any Ports | 1 IP<br>1 Port       | 0/24hrs      | No Hits                | ... |
| <input type="checkbox"/> | 6        | Block High Ports               | Enabled | Block  | Any Application                               | Any      | Any IPs<br>Any Ports | Any IPs<br>1 Port    | 0/24hrs      | No Hits                | ... |
| <input type="checkbox"/> | 7        | Default Rule                   | Enabled | Allow  | Any Application                               | Any      | Any IPs<br>Any Ports | Any IPs<br>Any Ports | 14.7 k/24hrs |                        | ... |

Edit
Duplicate
Logging
Allow

360062629451

2. ログインが有効になっている場合は、ネットワークトンネルが設定されているルータで次のコマンドを実行します。

<#root>

show crypto ikev2 sa

送信元IPアドレスが、RFC 1918に従ってユーザネットワークの内部IPアドレスであることを確認します。[ネットワークトンネル設定](#)のガイドに従って、設定を確認します。それでもエラーが解決しない場合は、サポートチームにサポートを依頼するために、CDFWログと一緒にshow crypto ikev2 saコマンドを実行し、チケットを作成してください。

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。